Location Verification and Smart Contracts

Location Verification and Smart Contracts

Ella Tallyn
University of Edinburgh
ella.tallyn@ed.ac.uk

Edson Alcala
University of Edinburgh
edson.alcala@ed.ac.uk

Dave Murray-Rust
University of Edinburgh
d.murray-rust@ed.ac.uk

Abstract

This paper explores the interactions between distributed ledgers, smart contracts and geographic location. Location is a fundamental part of human existence, as well as being crucial personally identifying information. We are interested in techniques for using location in smart contracts, to enable new kinds of services and systems, that link real world events to the abstract logics of blockchain systems. There are many challenges here, from the technical issues of sensing and securely storing location data, through to how to make use of the information in a privacy preserving manner, to developing a system of location appropriate for use in smart contracts. We discuss an experiment in progress to elicit a taxonomy of locations, and the important features of each. We then look at the techniques for capturing and storing this securely, and imagine how this feeds into the design of future active travel systems.

Introduction

Blockchain and distributed ledgers technologies (DLTs) are a potential route to enabling reliable and trustworthy platforms for sharing and storing data. In particular they are useful when it is necessary to verify stored data at a later time, as the cryptographic process by which data is compiled in these ledgers makes them highly tamper-resistant. Furthermore, these ledgers can be decentralised, and can be owned and managed by multiple organisations, none of

which could easily take control or manipulate the data for their own benefit. These attributes make DLTs particularly useful when certainty of the data is required, and where trust between the parties sharing data needs to be mediated [12, 15].

In this project we are exploring the ways in which DLTs can support proof of location, and allow the verification of location properties. Location verification is necessary in situations where the location of a particular object or person has significant implications, for example for shipping, insurance companies, and in legal situations. However monitoring location also has challenges, particularly around privacy [3], where the effects and implications of widespread location tracking are still being worked out [8]. Maintaining a sense of what is important to people and society is essential to preserving human values in technological development, particularly when it concerns the continual monitoring of our activities, and attention to this has been raised as a current concern by the HCI community [16]. Using a digital ledger for recording location data enables verification, whilst allowing the possibility of protecting privacy around sharing specific location. Blockchain has been explored for its potential to support minimal disclosure for identity management systems [6] and for access to medical records [9]. For verifying location, precisely notarized location data can be recorded, from which partial information regarding this location that is sufficient for the purpose can be released. This is known as attribute verification, and enables minimal disclosure, where only what is essential to a party seeking information is released. So, for example, an individual's driving data could be recorded across a 1-year period, and when they renegotiate their annual insurance policy, the insurance company could be provided with verification that this individual's driving has been within legal limits, but without knowing exactly where the individual has been.

Whilst digital ledgers are a good way to store this data when verification is required, smart contracts enable us to use this location data in connection with other events in the world. Smart contracts contain computational structures, with automated actions that will be executed in the event of certain conditions being met. This allows them to securely coordinate activity between multiple distributed agents (Figure 1).

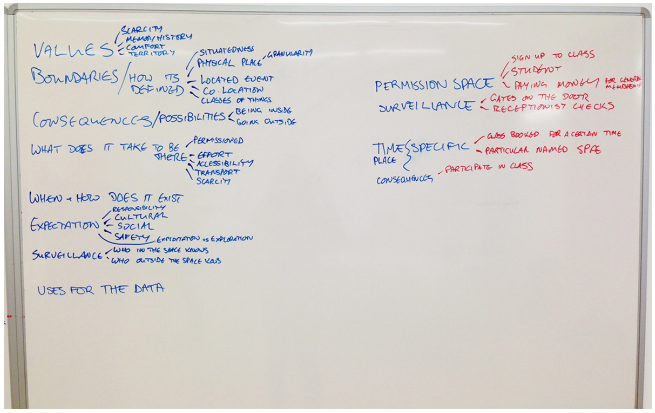

Figure 1: Location taxonomy generated in workshop

What is important about location?

In order to support privacy using the concept of minimal disclosure we are seeking to map out different types of location that are important in a variety of contexts and how these relate to privacy issues. Different types of space and the way that we relate to them has been studied in geographic disciplines [4]. Taxonomies of location have been constructed to underpin pervasive computing systems [5]. We need to understand what is important about location to individuals and more specifically, how this location might be useful to others, which aspects of location must be

concealed, and which are safe to reveal and in what situations. To do this we have asked 40 participants to record moments throughout their day when their location, or another person's or object's location, is important. We have already seen through an initial analysis of a location diary that what may be more important is trust in the information, rather than exact location data. For example an individual on a business trip arrives at a hotel and wants to check that her colleague has also arrived safely at the hotel. The hotel staff tell her that he has checked in. This gives her certainty that he has arrived safely and is therefore likely to make it on time to the meeting next day, although she doesn't need to know where he is right now. The data from the participants diaries has been used in a workshop context to begin development of a taxonomy of location types. This taxonomy will be used to inform technological innovation in this area. The first of these workshops has taken place and Figure 1 shows a taxonomy generated in the workshop drawn out of the location diaries and workshop participants' experiences.

Methods of verifying location data

Traditionally, devices need to know where they are in the world. There are several methods for doing this. GPS provides blanket coverage, at the cost of increased energy expenditure, and poor functionality in urban areas. There are a number of radio technologies for localization systems without the use of GPS. WiFi access points and their signal strengths are commonly used to get an idea of location. Bluetooth beacons can be used to provide a guaranteed location, even going as far as carrying out cryptographic exchanges that demonstrate a mobile device is close to the bluetooth hardware. Mobile phone cell towers can be used to triangulate GSM devices, and new networks such as LORA can locate IoT devices at an infrastructure level. Location systems that rely on honest devices can be spoofed, for example users modifying the location data sent from their phones. Systems that involve background infrastructure are typically harder to spoof: a device cannot arbitrarily fake being close to a cryptographically secure beacon. However, even here, multiple devices may be able to collude, and report verifications obtained by another device, and of course it require the background infrastructure to be present.

In terms of storage, there is a default option to write timestamped latitude and longitude position information into a database. However, in the interest of protecting privacy, other interesting possibilities can be explored, such as storing hashes of the location to allow verification without sharing the full location, or traces relative to an unknown origin, allowing properties such as distance or velocity to be determined, without storing the true location. For location points, GeoHashes offer a compact representation, well suited to blockchains, with structural properties that ensure truncated hashes contain all of their sub hashes - for example, Edinburgh's location (55.953251N, -3.188267E) hashes to `gcvwr3yr7czz`. A low precision version of this hash e.g. `gcvwr` shares a prefix with the hash for Leith (a region of Edinburgh), which is `gcvwrnu7sq84`. Hence, string comparisons can be used to efficiently compute containment and proximity.

For verifying the location of devices, peer to peer methods exist [2] where bluetooth connections between mobile devices allow a web of trust to be built up. Some more ecosystemic approaches are emerging, such as Sikorka [1], which combines GPS location with geospatial human intelligence tasks that require presence at a particular location—a user might be prompted for the name of the current ex-

[1] http://sikorka.io/

hibition, proving that they have line of sight. Finally, an integrated, decentralised approach to the entire question of location is being investigated by FOAM (foam.space), where location cells using LPWAN hardware mine triangulations to produce a background mesh of location driven blockchain systems. This is based on three components: i) a crypto-spatial coordinate system, using geohashes; ii) an incentivised peer-to-peer proof of location network; and iii) a spatial index that allows data and smart contracts to be spatially located and navigated.

Location Verification for Active Travel

Verified location data is attractive to a range of developing sectors and services, such as autonomous vehicles and supply chain tracking, and is being researched in these contexts e.g. [10, 7]. Blockchain technology has already been employed by a number of new commercial organisations, e.g. Provenance.org verifies supply chains, in order to build trust between stakeholders. Proof of location allows this to extend further into Digital Civics [17], enabling the development of a host of new potential systems and services which may bring radical transformation to the way we live. In particular, the combination of IoT and blockchains can inspire new approaches to creating sustainable transport systems in cities.

In recent years there has been an explosion of bicycle schemes in cities that use location tracking to gain a number of benefits. Recently, dockless schemes have become popular, using location tracking so that bikes can be locked and left at a place of the rider's convenience (e.g. Mobike, OBike, Urbo). These schemes need to manage rider behaviour around bicycle return, e.g. Mobikes incentivises riders to drop bikes at desirable locations, and penalises them for dropping them where they should not. In a slightly different proposition, See.Sense (seesense.cc), has built a bicycle light with location tracking for theft detection and location sensitive safety, that also shares anonymised to feed into civic improvements for cycling. As is common, data collected from these schemes is centralised, limiting its re-use value and making verification difficult.

Smart contracts for location aware objects

Thinking further ahead, we consider the application of a more radical use of these emerging technologies. Explorations of the future potential of digital ledgers and smart contracts has given rise to the somewhat abstract concept of distributed autonomous organisations or DAOs. Currently explored through digital art and thought pieces [2], DAOs are underpinned by digital ledgers with cryptocurrencies which enable objects to own a digital wallet. Digital wallets can be used to trade the cryptocurrencies associated with digital ledgers, and this means machines and systems can trade autonomously without recourse to human identity e.g. [14]. This raises the prospect of autonomous organisations run by algorithms rather than a centralised figure, and is seen as having the potential to provide more transparency and challenge current models of ownership and power [13].

As an example, "The Incredible Machine" —a team of 4 industrial designers exploring novel technologies through proposing radical new products—explored a bicycle DAO in a project called "Fairbike" [3]. Fairbike is self-owned and managed, and grows according to its use. Each bike owns itself and riders pay the bicycle for their journeys. The bicycle is able to contract local shops for repairs, buy a new bicycle with profits to expand the network, or decommission itself if it is no longer being used. The aim of this project is to create a not-for-profit, socially responsible alternative to

[2] e.g. http://okhaos.com/plantoids/ or http://digicult.it/news/terra0-la-foresta-aumentata-indipendente/

[3] https://the-incredible-machine.com/fairbike.html

existing dockless schemes. In this example, the distributed ledger handles payment as well as the data used to underpin the system, making it verifiable and transparent. This enables a complex system of actors who develop the system, the physical bikes and infrastructure necessary for their use and upkeep, and the users of this system who support and ultimately crowdfund the platform as they use it [11].

In this example, bicycle's location is not securely tracked, and adding a location aware infrastructure would bring many benefits. If a bicycle knows its location it could incentivise riders to store it in sheltered places, and contact the nearest bicycle shop for a regular service, incentivising its transport there. A DAO bicycle could explain its own value, using its usage data to demonstrate a contribution to meeting carbon reduction targets. This could be linked to systems of incentives for active travel, employing local services for bike maintenance, or providing open data on cycling, which could be used by a variety of organisations to improve cycling experience by improving infrastructure of other cycling services. Secure location data could act as a linkage between different systems. Multiple independent, distributed DAO cycle schemes and other active travel possibilities could be woven together into a transport ecosystem, offering riders a joined-up experience across the different schemes.

There are challenges here. Autonomous systems are not widespread, and there are no clear guidelines on how to design something that is robust, both with respect to keeping the system functioning, and against bad actors in the system [1]. Bicycles are dependent on people around them, in order to survive on the street, and the social mechanisms to make this work are largely untested. The sharing of personal information on blockchains is also in its infancy, and preserving privacy whilst enabling useful linkages between systems is an open challenge. Many possible solutions arise from exploring different data combinations, for example, a bicycle may not know its exact location, but instead may know if its in a good location for picking up its next rider, or a bicycle may know where it is, but not who is riding it. However, the ontology and risk surfaces of different location properties has not been fully articulated. Enabling possibilities such as knowing when a bicycle is near, or incentivising active travel through having provable carbon neutral journeys need to be balanced with the risks of accidental disclosure or identification. Gaining an understanding of different sorts of location that might be useful in different contexts and how these can be securely recorded into a ledger system to support minimal disclosure is essential to developing technology in this area.

Conclusion

Location verification has the potential to improve on existing services in sectors such as transport and shipping, but it also presents the possibility of inventing radical new solutions to problems such as urban congestion. Whilst the technology is still nascent, the potential challenges and benefits are becoming clear. What is required is a resilient, ecosystemic approach to the location identification, storage and verification that will enable maximum benefits whilst preserving the privacy and safety of its users. We need to understand the kinds of location that are appropriate in different situations, and develop a way to use these within smart contracts. This can lead to a system of minimal disclosure, where only the necessary location is shared, to support novel services while maintaining privacy. Whilst it is easy to envisage the social good that can come from sharing location based data across a range of different organisations to drive civic improvement, care needs to be taken to consider attitudes to privacy and trust, to encourage par-

ticipation in data driven systems. Ultimately it is important that we can harness these new technologies to support, rather than erode, existing trust and goodwill.

REFERENCES

1. 2016. A $50 Million hack just showed that the DAO was all too human. *Wired* (2016). https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/
2. Giacomo Brambilla, Michele Amoretti, and Francesco Zanichelli. 2016. Using Block Chain for Peer-to-Peer Proof-of-Location. *CoRR* abs/1607.00174 (2016). http://arxiv.org/abs/1607.00174
3. A.J. Bernheim Brush, John Krumm, and James Scott. 2010. Exploring End User Preferences for Location Obfuscation, Location-based Services, and the Value of Location. In *Proceedings UbiComp '10*. ACM, New York, NY, USA, 95–104.
4. Clare Davies, Chao Lili Li, and Jochen Albrecht. 2010. Human understanding of space. *Interacting with geospatial technologies* (2010), 19–35.
5. Simon Dobson. 2005. Leveraging the Subtleties of Location. In *Proceedings of the 2005 Joint Conference on Smart Objects and Ambient Intelligence: Innovative Context-aware Services: Usages and Technologies (sOc-EUSAI '05)*. ACM, New York, NY, USA, 189–193. DOI:http://dx.doi.org/10.1145/1107548.1107597
6. Paul Dunphy and Fabien AP Petitcolas. 2018. A First Look at Identity Management Schemes on the Blockchain. *arXiv preprint arXiv:1801.03294* (2018).
7. Marcus Foth. 2017. The Promise of Blockchain Technology for Interaction Design. In *Proceedings of OZCHI 2017*. ACM, New York, NY, USA, 513–517.
8. Alex Hern. 2018. Fitness tracking app Strava gives away location of secret US army bases. *The Guardian* (2018). https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
9. Thaís Bardini Idalino, Dayana Spagnuelo, and Jean Everson Martina. 2017. Private Verification of Access on Medical Data: An Initial Study. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 86–103.
10. Ao Lei, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P Anyigor Ogah, and Zhili Sun. 2017. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal* 4, 6 (2017), 1832–1843.
11. Ann Light and Jo Briggs. 2017. Crowdfunding Platforms and the Design of Paying Publics. In *Proceedings of CHI 2017*. ACM, New York, NY, USA, 797–809.
12. Caitlin Lustig and Bonnie Nardi. 2015. Algorithmic Authority: The Case of Bitcoin. In *Proceedings of HICSS 2015*. IEEE Computer Society, Washington, DC, USA, 743–752.
13. Bettina Nissen, Kate Symons, Ella Tallyn, Chris Speed, Deborah Maxwell, and John Vines. 2017. New Value Transactions: Understanding and Designing for Distributed Autonomous Organisations. In *Proceedings of DIS 2016*. ACM, 352–355.
14. Larissa Pschetz, Ella Tallyn, Rory Gianni, and Chris Speed. 2017. BitBarista: Exploring Perceptions of Data Transactions in the Internet of Things. In *Proceedings of CHI 2017*. ACM, 2964–2975.

15. Corina Sas and Irni Eliana Khairuddin. 2015. Exploring Trust in Bitcoin Technology: A Framework for HCI Research. In *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15)*. ACM, New York, NY, USA, 338–342.

16. Abigail Sellen, Yvonne Rogers, Richard Harper, and Tom Rodden. 2009. Reflecting Human Values in the Digital Age. *Commun. ACM* 52, 3 (March 2009), 58–66.

17. Vasillis Vlachokyriakos, Clara Crivellaro, Christopher A. Le Dantec, Eric Gordon, Pete Wright, and Patrick Olivier. 2016. Digital Civics: Citizen Empowerment With and Through Technology. In *Proceedings of CHI, Human Factors in Computing Systems 2016 (CHI EA '16)*. ACM, New York, NY, USA, 1096–1099.